PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-134260
(43)Date of publication of application : 20.05.1997

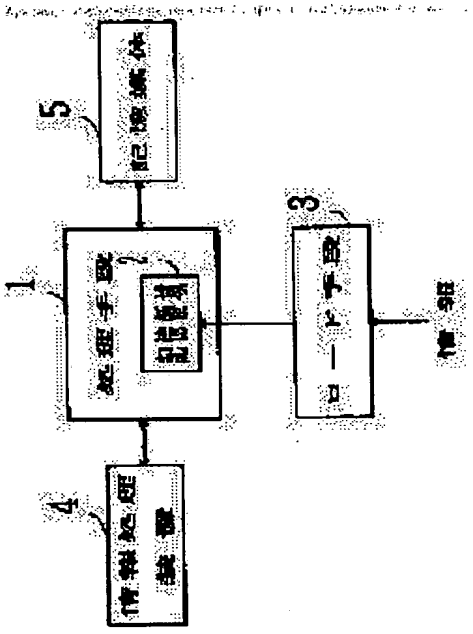
(51)Int.Cl. G06F 3/06
G06F 9/06

(21)Application number : 07-288932
(22)Date of filing : 07.11.1995

(71)Applicant : FUJITSU LTD
(72)Inventor : KOTANI MASATAKE
MURAKAMI KEIICHI
YOSHIMOTO SHINICHI
KANEMOTO KOICHI
MASUDA TATSURO
YOSHIOKA MAKOTO
FUJIWARA MASAO

(54) MEDIUM CONTROL METHOD AND DEVICE HAVING SECURITY FUNCTION

(57)Abstract:
PROBLEM TO BE SOLVED: To attain the loading of a processing program and to flexibly protect the security of information stored in a loaded medium by adding a rewritable area to the processing part of an external storage.
SOLUTION: A medium controller is provided with a processing means 1 and a loading means 3 and contained in an external storage. Then the medium controller performs the processing concerning the transfer of data between an information processor 4 and a storage medium 5. The medium 1 has a rewritable storage means 2 and performs the processing concerning the protection of the storage contents of the medium 5 based on the information stored in the area 2. The means 3 loads the information into the area 2 of the means 1. Thus the processing program to be carried out by the means 1 can be loaded and the storage contents of the medium 5 can be flexibly protected owing to the presence of the area 2 and the means 3 of the medium controller.



LEGAL STATUS

[Date of request for examination] 24.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－134260

(43)公開日　平成９年(1997)５月20日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	3/06	３０４		Ｇ０６Ｆ	3/06	３０４Ｈ
	9/06	５５０			9/06	５５０Ｘ

審査請求　未請求　請求項の数15　ＯＬ　（全 12 頁）

(21)出願番号　特願平7－288932

(22)出願日　平成７年(1995)11月７日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　村上　敬一
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

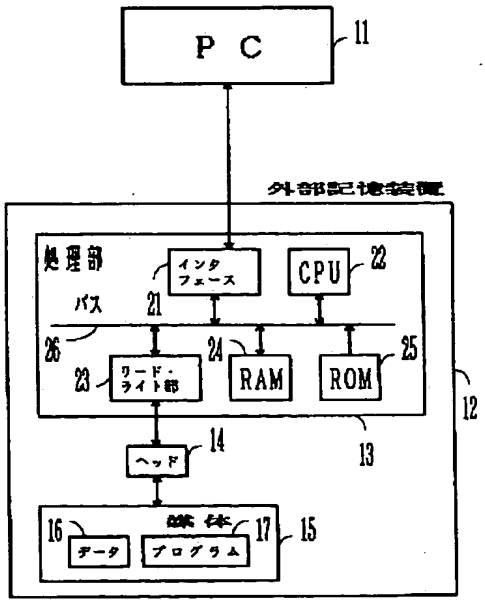
(74)代理人　弁理士　大菅　義之　（外１名）

最終頁に続く

(54)【発明の名称】　セキュリティ機能を有する媒体制御装置および方法

(57)【要約】
【課題】　取り外し可能な記憶媒体への不正なアクセスをリーズナブルなコストで防止することを課題とする。
【解決手段】　外部記憶装置１２の処理部１３はＲＡＭ（ランダムアクセス・メモリ）２４を備え、その内容はローダブルである。ＣＰＵ（中央処理装置）２２は、インタフェース２１やリード・ライト部２３を介してＲＡＭ２４にロードされたプログラムを用いて、ＰＣ（パーソナル・コンピュータ）１１と媒体１５の間のデータの授受に関する処理を行う。そして、媒体１５へのアクセスの可否を判定したり、暗号化されたデータ１７を復号したりする。ＲＡＭ２４の内容を書き換えることにより、フレキシブルで効率的な記憶内容の保護が実現される。

実施形態の構成図



1

【特許請求の範囲】

【請求項１】　取り外し可能な記憶媒体と組み合わせて使用され、該記憶媒体の記憶内容に関する処理を行う外部記憶装置において、

書き換え可能な記憶領域を有し、該記憶領域に格納された情報を利用して、前記記憶媒体の記憶内容の保護に関する処理を行う処理手段と、

前記記憶領域に前記情報をロードするロード手段とを備えることを特徴とする媒体制御装置。

【請求項２】　前記処理手段は、前記記憶領域にアクセス判定アルゴリズムを記憶し、該判定アルゴリズムを用いて、前記外部記憶装置が前記記憶媒体にアクセス可能か否かの判定を行うことを特徴とする請求項１記載の媒体制御装置。

【請求項３】　前記記憶媒体がローダブルなプログラムを搭載しているとき、前記ロード手段は該プログラムを前記記憶領域にロードし、前記処理手段は該プログラムを用いて該記憶媒体内のデータへのアクセスに関する処理を行うことを特徴とする請求項１記載の媒体制御装置。

【請求項４】　前記処理手段は、前記記憶媒体内に保持されたメディア識別記号を用いて、前記外部記憶装置が該記憶媒体にアクセス可能か否かのアクセス判定を行うことを特徴とする請求項１記載の媒体制御装置。

【請求項５】　取り外し可能な記憶媒体と組み合わせて使用され、該記憶媒体の記憶内容に関する処理を行う外部記憶装置において、

前記記憶媒体内に保持されたメディア識別記号および許諾記号を読み出すリード手段と、

該メディア識別記号を用いて判定記号を作成し、該判定記号を前記許諾記号と比較して、前記外部記憶装置が該記憶媒体にアクセス可能か否かのアクセス判定を行う処理手段とを備えることを特徴とする媒体制御装置。

【請求項６】　前記処理手段は、前記判定記号が前記許諾記号と一致した場合に、アクセス可能であると判定することを特徴とする請求項５記載の媒体制御装置。

【請求項７】　前記処理手段は、前記外部記憶装置内に保持された装置識別記号を読み出し、前記メディア識別記号および該装置識別記号を用いて前記判定記号を作成することを特徴とする請求項５記載の媒体制御装置。

【請求項８】　前記判定記号が前記許諾記号と一致しなかった場合、前記処理手段は、前記メディア識別記号を用いて所定の記号を作成し、該所定の記号を前記許諾記号と比較し、該所定の記号と前記許諾記号が一致すれば前記記憶媒体内の該許諾記号を前記判定記号に置き換えて、置き換えられた許諾記号を該判定記号と比較することにより、前記アクセス判定を行うことを特徴とする請求項５記載の媒体制御装置。

【請求項９】　前記処理手段は、前記所定の記号として、前記記憶媒体の供給者が該記憶媒体内に前記許諾記号として設定した供給者保証記号を作成することを特徴とする請求項８記載の媒体制御装置。

2

【請求項１０】　前記処理手段は、前記所定の記号として、前記記憶媒体のユーザが該記憶媒体内に前記許諾記号として設定した特殊記号を作成することを特徴とする請求項８記載の媒体制御装置。

【請求項１１】　前記処理手段は、前記所定の記号と前記許諾記号が一致しなかった場合に、アクセス不可能であると判定することを特徴とする請求項８記載の媒体制御装置。

【請求項１２】　前記処理手段は、前記記憶媒体内に保持された複数の許諾記号を順に前記所定の記号と比較し、該所定の記号と一致した許諾記号を前記判定記号に置き換えて、置き換えられた許諾記号を該判定記号と比較することにより、前記アクセス判定を行うことを特徴とする請求項８記載の媒体制御装置。

【請求項１３】　取り外し可能な記憶媒体と組み合わせて使用され、該記憶媒体の記憶内容に関する処理を行う外部記憶装置であって、

書き換え可能な記憶領域を有し、該記憶領域に格納された情報を利用して、前記記憶媒体の記憶内容の保護に関する処理を行う処理手段と、

前記記憶領域に前記情報をロードするロード手段とを備えることを特徴とする外部記憶装置。

【請求項１４】　外部記憶装置に装着されて使用される取り外し可能な記憶媒体であって、

メディア識別記号を保持するメディア識別記号領域手段と、

前記外部記憶装置が前記記憶媒体にアクセス可能か否かを判定するアクセス判定において、前記メディア識別記号を用いて作成される判定記号と比較される許諾記号を保持する許諾記号領域手段とを備えることを特徴とする記憶媒体。

【請求項１５】　外部記憶装置内の書き換え可能な記憶領域に情報をロードし、

該記憶領域にロードされた該情報を利用して、前記外部記憶装置に装着された記憶媒体の記憶内容の保護に関する処理を行うことを特徴とする媒体制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は取り外し可能な記憶媒体に係り、その記憶内容のセキュリティを保つ機能を持つ媒体制御装置およびセキュリティを保証する記憶媒体の制御方法に関する。

【０００２】

【従来の技術】情報処理技術の分野において、情報を記録する記憶媒体にはいくつかの種類のものがある。従来より用いられている取り外し可能な記憶媒体としては、磁気テープ、磁気ディスク、光磁気ディスク、光ディスク等が知られており、今日ではますます多様化する傾向

にある。

【０００３】近年、このような可搬性のある記憶媒体の大容量化によって、大量の情報を収納、供給、分配することが可能となってきている。これに伴い、記憶された情報のセキュリティをどのように保証するか、あるいは記憶された著作物の著作権の保護をどのように保証するかについて、関心が高まっている。

【０００４】情報のセキュリティや著作権の保護等は、情報の完全な囲い込みによって達成可能である。しかしながら、情報を完全に囲い込むシステムを構築するには、多大なコストを要する。また、取り外し可能な記憶媒体に対して、紛失、盗難等の危険性を零にすることは事実上不可能である。

【０００５】

【発明が解決しようとする課題】従来の可搬性記憶媒体内の情報のセキュリティ保護に関しては、次のような問題がある。

【０００６】取り外し可能な記憶媒体が、過失あるいは不正な手段等により、他の悪意ある人々の手に渡るのを完全に封じることは不可能である。記憶媒体が何等かのルートで悪意ある人の手に渡った場合、その媒体内の情報に対してその人がアクセス可能であるならば、その情報のセキュリティや著作権の保護等は保証されない。したがって、そのような事態において、媒体内の情報への不正なアクセスを不可能にすることが望まれる。

【０００７】本発明は、取り外し可能な記憶媒体への不正なアクセスをリーズナブルなコストで防止できる媒体制御装置およびその方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】図１は、本発明の媒体制御装置の原理図である。図１の媒体制御装置は処理手段１とロード手段３を備え、外部記憶装置内に設けられる。そして、情報処理装置４と記憶媒体５の間のデータのやり取りに関する処理を行う。

【０００９】処理手段１は書き換え可能な記憶領域２を有し、その記憶領域２に格納された情報を利用して、記憶媒体５の記憶内容の保護に関する処理を行う。ロード手段３は、処理手段１の記憶領域２に上記情報をロードする。

【００１０】このように、媒体制御装置に書き換え可能な記憶領域２とロード手段３とを設けたことで、処理手段１が実行する処理プログラムがローダブルになり、記憶媒体５の記憶内容の保護をフレキシブルに行うことができる。

【００１１】例えば、ロード手段３がデータと対にして記憶媒体５内に記憶されたプログラムをロードし、処理手段１がそのプログラムを用いてデータへのアクセスに関する処理を行う。これにより、データ毎にまたは媒体毎に異なるアクセスアルゴリズムや暗号化アルゴリズムを採用することが可能になる。

【００１２】また、処理手段１は、記憶領域２にアクセス判定アルゴリズムを記憶し、それを用いて、外部記憶装置が記憶媒体５にアクセス可能か否かの判定を行う。判定アルゴリズムの一例として、記憶媒体５とその記憶内容にアクセスできる外部記憶装置とを対にすることをある段階で許諾し、それ以外の組合せにおいては媒体へのアクセスを禁止する方法を用いる。

【００１３】この方法によれば、許諾された記憶媒体と外部記憶装置の対においてのみ、記憶内容へのアクセスが許可される。このため、過失や故意によって他の対が形成された場合に、アクセスを禁止することができ、記憶内容のセキュリティや著作権の保護等が保証される。

【００１４】例えば、図１の処理手段１は実施形態における図２の処理部１３に対応し、記憶領域２はＲＡＭ（ランダムアクセス・メモリ）２４に対応し、ロード手段３はインタフェース２１またはリード・ライト部２３に対応する。また、情報処理装置４は、例えばパーソナルコンピュータ（ＰＣ）１１に対応する。

【００１５】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態を詳細に説明する。図２は、実施形態の情報処理システムの構成図である。図２の情報処理システムは、ＰＣ１１と外部記憶装置１２を備える。

【００１６】外部記憶装置１２は、装着された媒体１５へのアクセスを行うヘッド１４と、それを制御するためのドライブ処理を行う処理部１３を備え、ＰＣ１１からの指示等に基づいて媒体１５の記憶内容をアクセスする。媒体１５には、例えば、データ１６とローダブルなプログラム１７が格納されている。プログラム１７は、例えば、データ１６をアクセスするために必要なアルゴリズムを含み、データ１６が暗号化されている場合は、さらにその復号アルゴリズムも含む。

【００１７】処理部１３は、インタフェース２１、ＣＰＵ（中央処理装置）２２、リード・ライト部２３、ＲＡＭ２４、ＲＯＭ（リードオンリー・メモリ）２５、およびそれらを結合するバス２６を備え、ＰＣ１１と通信しながら媒体１５へのアクセス処理を行う。

【００１８】インタフェース２１はＰＣ１１との間で情報のやり取りを行い、リード・ライト部２３はヘッド１４を制御して、媒体１５の記憶内容を読み出したり、媒体１５への書き込みを行ったりする。ＣＰＵ２２は、ＲＡＭ２４やＲＯＭ２５内の情報を用いてドライブ処理を行う。例えば、ＣＰＵ２２としてはマイクロ・プロセッサが用いられ、処理部１３はマイクロ・コンピュータとして構成される。

【００１９】ＲＯＭ２５には、外部記憶装置１２の電源投入（パワーオン）時に実行されるドライブ処理のプログラムがあらかじめ格納されている。また、ＲＡＭ２４には、外部記憶装置１２が媒体１５にアクセス可能か否かの判断を行うプログラムが格納され、ＣＰＵ２２はそ

のアルゴリズムを用いてアクセス判定を行う。ＲＡＭ２４内のプログラムがデータ１６の復号アルゴリズムを含む場合は、ＣＰＵ２２はそれを用いてデータ１６を復号する。

【００２０】ＲＡＭ２４内のプログラムは、インタフェース２１やリード・ライト部２３を介してロードした情報を用いて書き換えることができ、そのアルゴリズムは可変（ローダブル）である。処理部１３へのプログラムのローディング方法としては、例えば、媒体１８やＰＣ１１からロードしてＲＡＭ２４に格納する方法がある。そのほかにも、ＲＯＭ２５にプログラムを書き込んでおき、変更時にはＲＯＭ２５ごと交換するなど、種々の方法が考えられる。

【００２１】次に、図３から図５までを参照しながら、データ１６が暗号化されている場合に、それを読み出して復号するドライブ処理について説明する。図３は、処理部１３の動作フローチャートである。図３において、外部記憶装置１２に電源が投入されると（ステップＳ１）、ＣＰＵ２２は、ＲＯＭ２５内のプログラムによるドライブ処理を行い（ステップＳ２）、電源がオフになると（ステップＳ３）、処理を終了する。

【００２２】図４は、図３のステップＳ２で行われる媒体判別処理のフローチャートである。図４において処理が開始されると、処理部１３は、ヘッダ１４からの情報を元に外部記憶装置１２に媒体１５がセットされたかどうかを判定する（ステップＳ１１）。媒体１５がセットされていなければこの判定を繰り返し、媒体１５がセットされれば、その所定領域のデータを読み取る（ステップＳ１２）。

【００２３】そして、媒体１５がロード可能（ローダブル）なプログラムを搭載していることを、そのデータが示しているかどうかを判定する（ステップＳ１３）。読み取ったデータがローダブルなプログラムの搭載を示していれば、媒体１５からそのプログラム１７を読み出してＲＡＭ２４に格納し（ステップＳ１４）、そのプログラム１７に基づく復号処理を行って（ステップＳ１５）、処理を終了する。

【００２４】また、媒体１５がローダブルなプログラムを搭載していないと判定されれば、あらかじめＲＡＭ２４に格納されていたプログラムに基づく復号処理を行って（ステップＳ１５）、処理を終了する。

【００２５】図５は、図４のステップＳ１５で行われるデータ１６の復号処理のフローチャートである。図５において処理が開始されると、処理部１３は、まずＰＣ１１からデータ１７のリード要求とともに暗号解読用のキーを受け取る（ステップＳ２１）。

【００２６】次に、媒体１５中の暗号化されたデータ１６を読み出し（ステップＳ２２）、ＲＡＭ２４内のプログラム１７のアルゴリズムに従い、キーを用いてデータ１６を復号する（ステップＳ２３）。このとき、例えば、プログラム１７に定められた変換式中の変数にキーを代入して、データ１６の変換を行う。そして、復号されたデータをＰＣ１１に渡して（ステップＳ２４）、処理を終了する。

【００２７】このように、データ１６と対にして格納されたプログラム１７を用いて復号処理を行うなうことで、データ毎または媒体毎に異なる復号アルゴリズムを用いることができるようになる。

【００２８】次に、図６から図１１までを参照しながら、処理部１３による装着媒体へのアクセス判定処理について説明する。図６は、アクセス判定を行う場合の情報処理システムの構成図である。図６において、基本的に図２と同様の構成要素には同じ符号が付けられている。ＰＣ１１は、ユーザのアプリケーション・プログラム３１と、外部記憶装置１２にアクセスするためのソフトウェアツールであるデバイスドライバ３２を有する。また、外部記憶装置１２の処理部１３は、ドライブ識別記号（ＤＩＤ：drive identifier）を記憶するＤＩＤ記憶部３３を備える。

【００２９】ＤＩＤは、外部記憶装置１２のドライブをユニークに限定することのできる装置識別記号であり、例えば外部記憶装置１２の製造時のシリアル番号、またはこれに類する記号等が用いられる。このＤＩＤは書き換え不可能であることが望ましく、ＤＩＤ記憶部３３は、例えばＲＯＭ２５内に設けられる。

【００３０】媒体３４内には、メディア識別記号（ＭＩＤ：medium identifier）を記憶するＭＩＤ領域３５と、許諾記号（ＬＣ：license code）を記憶するＬＣ領域３６が設けられる。

【００３１】ＭＩＤは、媒体３４をユニークに限定することのできる識別子であり、書き換え不可能な方法で媒体に書き込まれることが望ましい。このため、ＭＩＤ領域３５は、媒体３４内の書き換え不可能な部分に設けられる。そのほかに、例えば論理的パリティチェックを多用して記号構造を複雑にするなど、書き換えに多大のコストを要する方法を用いて、ＭＩＤを書き込んでもよい。

【００３２】また、ＬＣ領域３６は媒体３４内の書き換え可能な部分に設けられ、処理部１３が媒体３４へのアクセスの可否を判定する際に用いられる。処理部１３は、アクセス判定において、必要に応じてＬＣを書き換えることができる。ただし、ＰＣ１１内のアプリケーション・プログラム３１やデバイスドライバ３２は、このＬＣ領域３６にアクセスすることはできない。

【００３３】以下の実施形態で用いる判定アルゴリズムによれば、媒体３４とその記憶内容にアクセスできる外部記憶装置１２とを対にすることをある段階で許諾し、それ以外の組合せにおいては媒体へのアクセスができないようにする。そのために、処理部１３は媒体３４上のＭＩＤと外部記憶装置１２上のＤＩＤからユニークに決

められる判定記号（ＪＣ：judge code）を生成する。そして、ＬＣとＪＣを用いてアクセス判定を行う。

【００３４】図７は、処理部１３による第１のアクセス判定処理のフローチャートである。図７において処理が開始されると、処理部１３は、まずＤＩＤ記憶部３３からＤＩＤを読み出し（ステップＳ３１）、媒体３４からＭＩＤとＬＣを読み出す（ステップＳ２）。そして、第１の記号生成アルゴリズムに従ってＭＩＤとＤＩＤからＪＣを作成し（ステップＳ３３）、それをＬＣと比較する（ステップＳ３４）。作成したＪＣが媒体３４のＬＣと一致すれば、外部記憶装置１２による媒体３４へのアクセスが可能と判定し（ステップＳ３５）、処理を終了する。

【００３５】これ以降は、ＰＣ１１からの要求に従って、媒体３４にアクセスすることが可能になる。ステップＳ３４においてＪＣがＬＣと一致しなかった場合は、次に、第２の記号生成アルゴリズムに従ってＭＩＤから供給者保証記号（ＳＧＣ：supplier guarantee code）を作成し（ステップＳ３６）、それをＬＣと比較する（ステップＳ３７）。

【００３６】ＳＧＣは、媒体３４の出荷時に、その供給者により上記第２の記号生成アルゴリズムと同じアルゴリズムに従って生成され、媒体３４のＬＣ領域３６にＬＣの初期値として書き込まれている。処理部１３は、そのＳＧＣを作成して媒体３４上のＬＣと比較することにより、媒体３４のＬＣが出荷時のままであるかどうかを調べることができる。

【００３７】ここで、作成したＳＧＣがＬＣと一致すれば媒体３４はまだ新しいことが分かるので、媒体３４上のＬＣをＪＣに置き換え（ステップＳ３８）、ステップＳ３２以降の処理を繰り返す。この場合、ＬＣ領域３６内のＬＣはＪＣそのものであるので、ステップＳ３４においてＬＣとＪＣが一致し、アクセスが可能になる（ステップＳ３５）。

【００３８】一方、ＳＧＣとＬＣが一致しなかった場合は、外部記憶装置１２による媒体３４へのアクセスは不可能と判定し（ステップＳ３９）、処理を終了する。この場合には、ＬＣ領域３６にＳＧＣやＪＣ以外の記号、例えば他の記号生成アルゴリズムや他の装置のＤＩＤを用いて生成されたＪＣが書き込まれており、外部記憶装置１２の媒体３４へのアクセスが禁止される。

【００３９】このように、ＭＩＤとＤＩＤの両方を用いてＪＣを作成し、それをＬＣ領域３６に書き込むことにより、他のＤＩＤを持つ装置による媒体３４へのアクセスを禁止することができる。言い換えれば、媒体３４にアクセス可能な外部記憶装置１２がＬＣ領域３６に登録されることになる。

【００４０】尚、ステップＳ３３において、ＭＩＤのみを用いてＪＣを作成することにしてもよい。その場合も、他のシステムと異なる生成アルゴリズムでＪＣを作成すれば、同様の効果を得ることができる。

【００４１】以上の形態では、媒体３４は外部記憶装置１２以外の装置からはアクセス不可能になるが、ＬＣを複数書き込み可能な媒体を用いれば、それを複数の装置からアクセス可能にすることもできる。

【００４２】図８は、複数のＬＣを持つ媒体を示している。図８の媒体４１は、ＭＩＤを記憶するＭＩＤ領域４２と、ｎ個（ｎは１以上の整数）のＬＣに相当するＬＣ（１）、ＬＣ（２）、・・・、ＬＣ（ｎ）を記憶するＬＣ領域４３とを有する。これらのＬＣ（ｉ）（ｉ＝１，２，．．．，ｎ）にはあらかじめＳＧＣが書き込まれているが、各々のＳＧＣをＪＣへ書き換えることにより、最大ｎ個の異なるＤＩＤを持つ装置を登録することができる。

【００４３】図９および図１０は、媒体４１へのアクセスの可否を判定する第２のアクセス判定処理のフローチャートである。図９において処理が開始されると、処理部１３は、まずＤＩＤ記憶部３３からＤＩＤを読み出し（ステップＳ４１）、制御変数ｉを１とおく（ステップＳ４２）。

【００４４】次に、媒体４１からＭＩＤとＬＣ（ｉ）を読み出し（ステップＳ４３）、第１の記号生成アルゴリズムに従ってＭＩＤとＤＩＤからＪＣを作成して（ステップＳ４４）、それをＬＣ（ｉ）と比較する（ステップＳ４５）。作成したＪＣが媒体４１のＬＣ（ｉ）と一致すれば、外部記憶装置１２による媒体４１へのアクセスが可能と判定し（ステップＳ４６）、処理を終了する。

【００４５】ステップＳ４５においてＪＣがＬＣ（ｉ）と一致しなかった場合は、ｉをｎと比較する（ステップＳ４７）。そして、ｉがｎより小さければｉ＝ｉ＋１とおいて（ステップＳ４８）、ステップＳ４３以降の処理を繰り返す。

【００４６】ステップＳ４７においてｉがｎに達すると、ＪＣはいずれのＬＣ（ｉ）とも一致しなかったことが分かる。そこで、次に、第２の記号生成アルゴリズムに従ってＭＩＤからＳＧＣを作成し（図１０、ステップＳ４９）、再びｉ＝１とおく（ステップＳ５０）。

【００４７】次に、作成したＳＧＣをＬＣ（ｉ）と比較し（ステップＳ５１）、ＳＧＣがＬＣと一致すれば、媒体４１上のＬＣ（ｉ）をＪＣに置き換え（ステップＳ５２）、図９のステップＳ４２以降の処理を繰り返す。ステップＳ５１においてＳＧＣとＬＣ（ｉ）が一致しなかった場合は、ｉをｎと比較する（ステップＳ５３）。そして、ｉがｎより小さければｉ＝ｉ＋１とおいて（ステップＳ５４）、ステップＳ５１以降の処理を繰り返す。

【００４８】ステップＳ５３においてｉがｎに達すると、いずれのＬＣ（ｉ）にもＳＧＣが格納されておらず、新たな装置の登録は不可能であることが分かる。そこで、外部記憶装置１２による媒体４１へのアクセスは不可能と判定し（ステップＳ５５）、処理を終了する。

【００４９】このような第２のアクセス判定処理によれば、最大ｎまでの外部記憶装置に対して、媒体へのアクセスを許可することが可能になる。第１および第２のアクセス判定処理において、ＭＩＤを用いて生成される初期のＬＣの例として供給者が作成するＳＧＣを挙げたが、これ以外に、媒体の所有者が独自に作成した特殊記号（ＳＰＣ：special code）を用いることもできる。

【００５０】この場合、媒体の所有者は、そのＬＣ領域のＳＧＣをあらかじめユニークに決定されたＳＰＣに書き換えておき、その生成アルゴリズムを第２の記号生成アルゴリズムとして、ＰＣ１１からＲＡＭ２４内にロードしておく。そして、処理部１３は、図７のステップＳ３６や図１０のステップＳ４９において、そのアルゴリズムを用いてＳＰＣを作成し、ステップＳ３７やステップＳ４５において、ＳＰＣをＬＣやＬＣ（ｉ）と比較する。

【００５１】このようにＳＧＣの代わりにＳＰＣを用いれば、その生成アルゴリズムは、媒体の供給者を含めて所有者以外の誰も知らないことになる。したがって、装置が未登録の状態でも、所有者以外の装置は媒体にアクセスすることができなくなる。特に、媒体と装置とをシステム的に統合して運用する組織、例えば銀行においては、このようなＳＰＣを書き込んでおくことが有効である。この場合、ＳＰＣは、その組織の責任の元に決定され、使用される。

【００５２】ところで、アクセス判定のアルゴリズムは上述したようにＲＡＭ２４内に格納されており、必要に応じてその１部または全部を変更することが可能である。例えば、第１のアクセス判定処理において、ＪＣを作成する第１の記号生成アルゴリズムがＲＡＭ２４内で変更された場合、そのままでは媒体３４への以後のアクセスが不可能になる。そこで、アルゴリズムの変更を検出する処理が必要になる。

【００５３】図１１は、このような第１の記号生成アルゴリズムの変更に対応可能な第３のアクセス判定処理のフローチャートである。第３のアクセス判定処理の全体フローは、図７の第１のアクセス判定処理のフローに図１１の３つのステップを挿入して得られる。

【００５４】図７のステップＳ３４においてＪＣがＬＣと一致しなかった場合、処理部１３は、次に第１の記号生成アルゴリズムが変更されたかどうかを調べる（ステップＳ６１）。第１の記号生成アルゴリズムが変更されていなければステップＳ３６以降の処理に進み、媒体３４が新しいかどうかを調べる。

【００５５】それが変更されている場合は、変更前の記号生成アルゴリズムに従ってＭＩＤとＤＩＤからＪＣ′を作成し（ステップＳ６２）、それをＬＣと比較する（ステップＳ６３）。変更前の記号生成アルゴリズムは、その変更時に、旧アルゴリズムとしてＲＡＭ２４内に残されているものとする。

【００５６】ここで、作成したＪＣ′がＬＣと一致しなければステップＳ３６以降の処理に進み、媒体３４が新しいかどうかを調べる。両者が一致すれば、媒体３４に外部記憶装置１２が登録されていたことが分かるので、ステップＳ３８の処理に進み、ＬＣを変更後のアルゴリズムにより作成されたＪＣに置き換える。こうして、新しいアルゴリズムを用いて外部記憶装置１２が再登録される。

【００５７】以上の実施形態においては、外部記憶装置の処理部がＲＡＭに格納されたプログラムを用いて、復号処理やアクセス判定処理等の、媒体内の情報のセキュリティ保護に関する処理を行っている。このようなセキュリティに関する他の処理として、媒体内のデータの暗号化処理、コード変換処理、データ修飾処理等を行うことも可能である。さらに、処理部は、媒体とＰＣの間でやり取りされる情報のより一般的な加工処理を行うこともできる。

【００５８】

【発明の効果】本発明によれば、外部記憶装置の処理部に書き換え可能な領域を設けたことで、その処理プログラムがローダブルになり、装着された媒体内の情報のセキュリティ保護をフレキシブルに行うことができる。例えば、データと対にして媒体内に記憶されたプログラムをロードして、そのデータへのアクセスに関する処理を行うことができる。これにより、データ毎にまたは媒体毎に異なる暗号化アルゴリズムを採用することが可能になる。

【００５９】また、許諾された記憶媒体と記憶装置の対においてのみ、媒体の記憶内容へのアクセスを許可することが可能になり、過失、故意によって形成された他の対におけるデータへの不正なアクセスを禁止することができる。

【００６０】したがって、媒体内の情報のセキュリティや、その情報に関する著作権の保護等が効率的に保証される。

【図面の簡単な説明】

【図１】本発明の原理図である。

【図２】実施形態の構成図である。

【図３】処理部の動作フローチャートである。

【図４】媒体判別処理のフローチャートである。

【図５】復号処理のフローチャートである。

【図６】アクセス判定を行うシステムの構成図である。

【図７】第１のアクセス判定処理のフローチャートである。

【図８】複数のＬＣを持つ媒体を示す図である。

【図９】第２のアクセス判定処理のフローチャート（その１）である。

【図１０】第２のアクセス判定処理のフローチャート（その２）である。

【図１１】第３のアクセス判定処理のフローチャートで

11

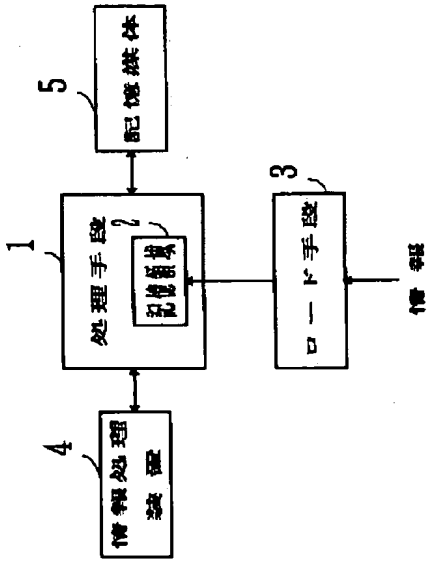
ある。

【符号の説明】

１　処理手段
２　記憶領域
３　ロード手段
４　情報処理装置
５、１５、３４、４１　記憶媒体
１１　パーソナルコンピュータ
１２　外部記憶装置
１３　処理部
１４　ヘッド
１６　データ
１７　プログラム

【図１】

本発明の原理図

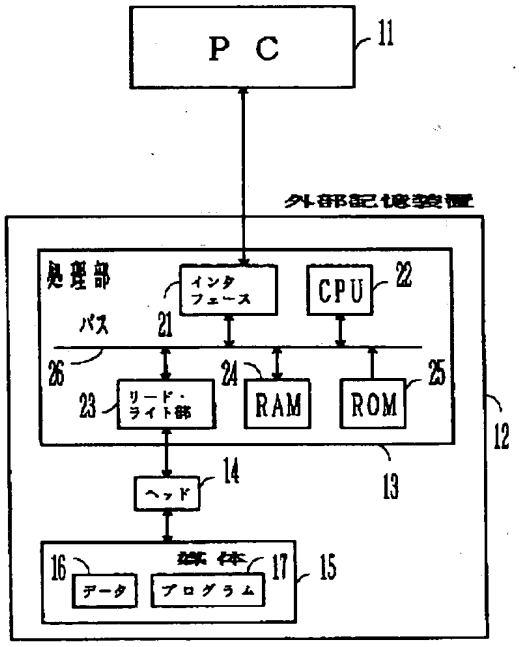


12

２１　インタフェース
２２　ＣＰＵ
２３　リード・ライト部
２４　ＲＡＭ
２５　ＲＯＭ
２６　バス
３１　アプリケーション・プログラム
３２　デバイスドライバ
３３　ＤＩＤ記憶部
３５　ＭＩＤ領域
３６　ＬＣ領域
４２　ＭＩＤ領域
４３　ＬＣ領域

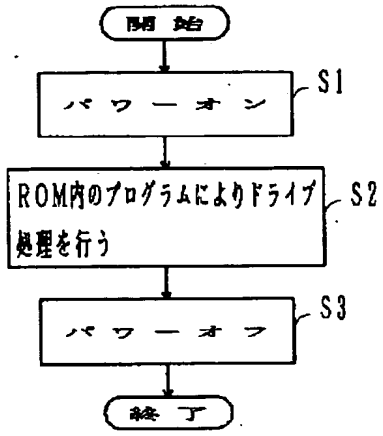
【図２】

実　施　形　態　の　構　成　図



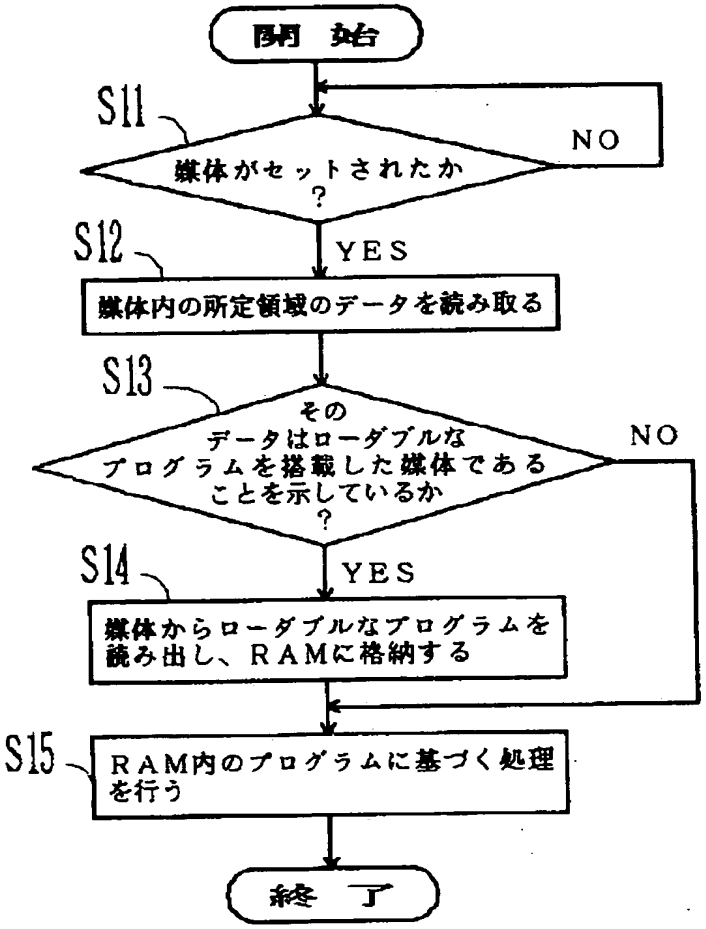
【図３】

処理部の動作フローチャート



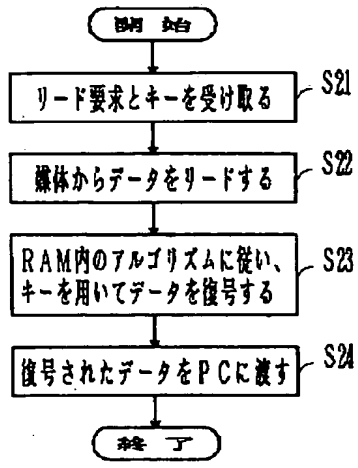
【図４】

媒体判別処理のフローチャート



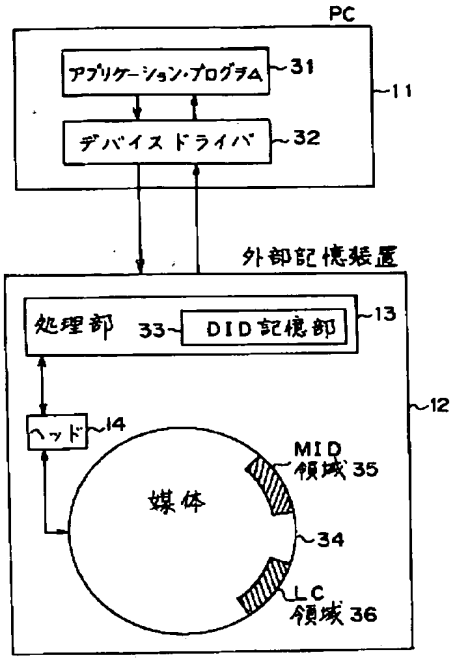
【図５】

復号処理のフローチャート



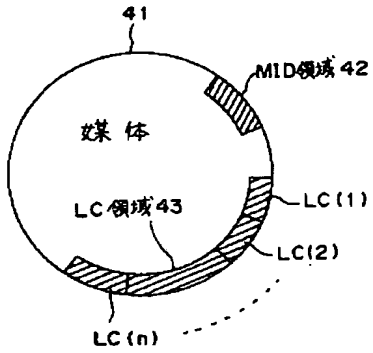
【図６】

アクセス判定を行うシステムの構成図



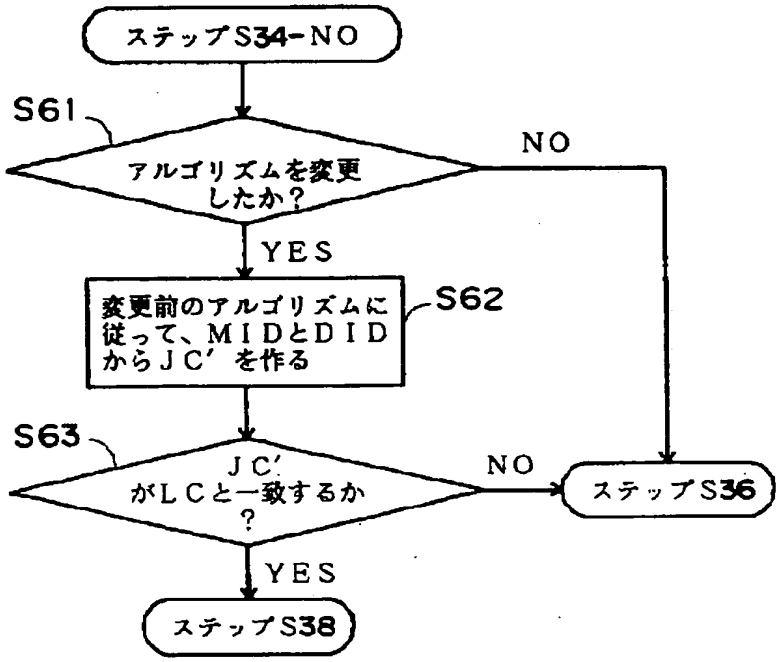
【図８】

複数のLCを持つ媒体を示す図



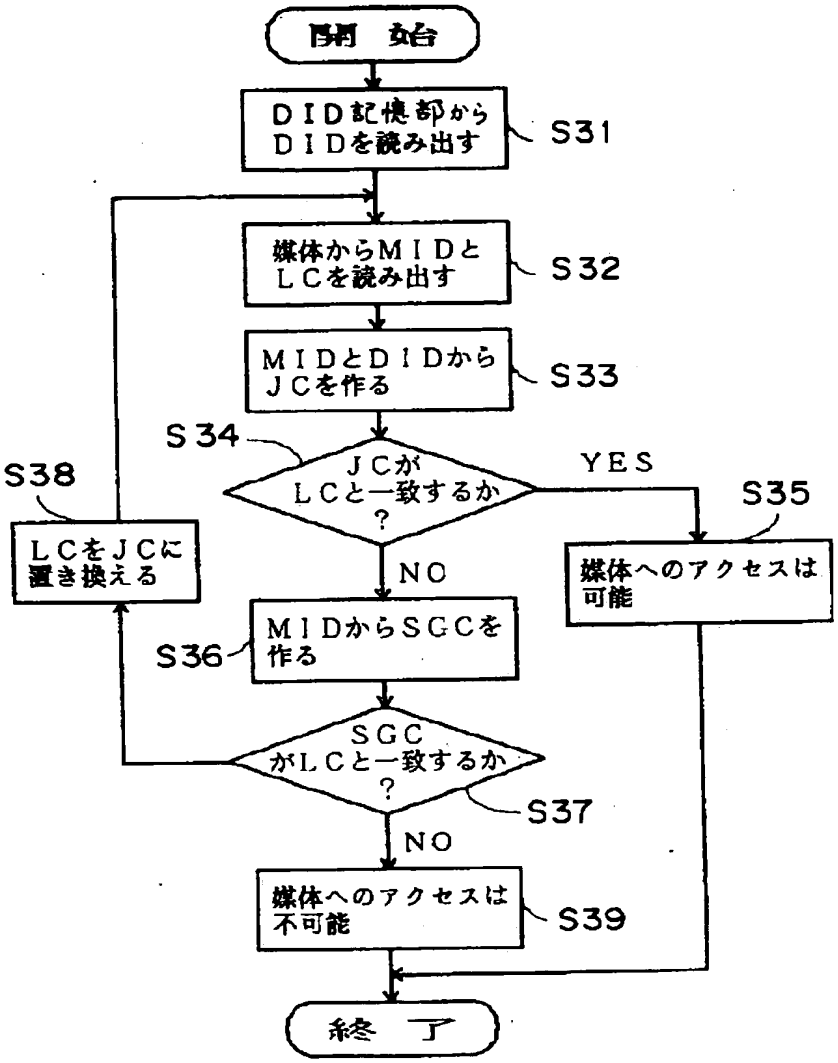
【図１１】

第３のアクセス判定処理のフローチャート



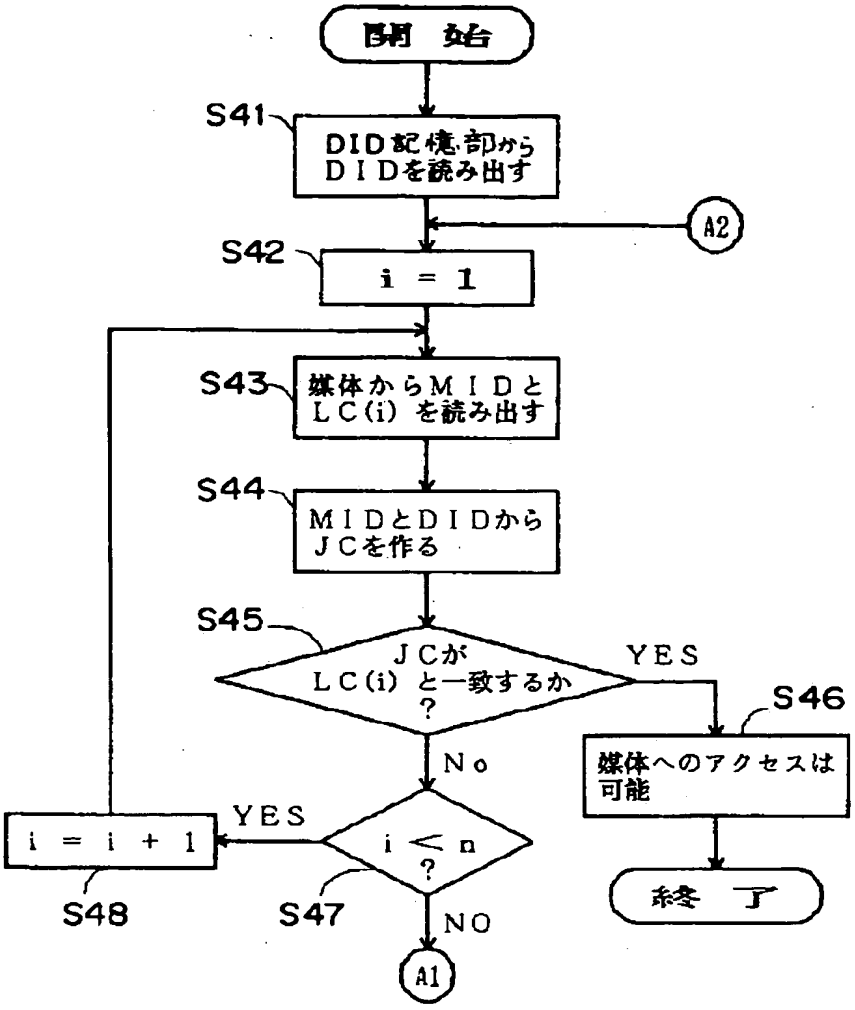
【図７】

第１のアクセス判定処理のフローチャート



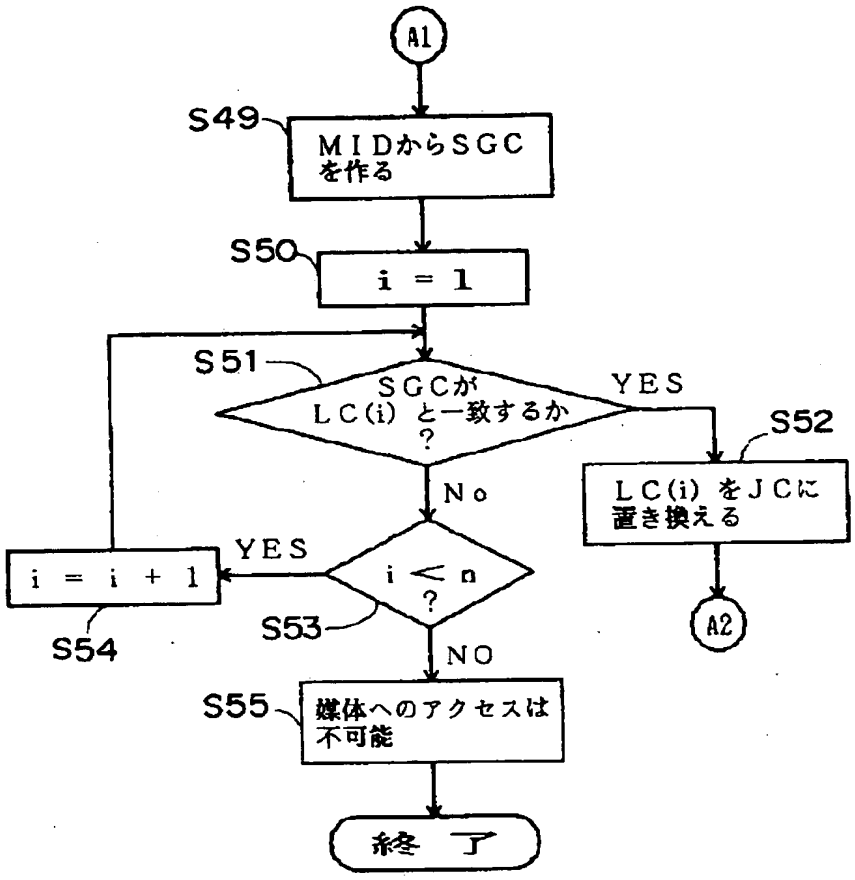
【図９】

第２のアクセス判定処理のフローチャート（その１）



【図１０】

第２のアクセス判定処理のフローチャート（その２）



フロントページの続き

(72)発明者　吉本　真一
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　金元　浩一
群馬県前橋市問屋町１丁目８番３号　株式会社富士通ターミナルシステムズ内

(72)発明者　増田　達朗
群馬県前橋市問屋町１丁目８番３号　株式会社富士通ターミナルシステムズ内

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　藤原　眞雄
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内